UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,600	07/26/2001	Chris A. Barton	NAI1P020/01.139.01	8707

28875 7590 06/23/2008

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/916,600
Filing Date: July 26, 2001
Appellant(s): BARTON ET AL.

Kevin J. Zilka
Reg. No. 41,429
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/05/2006

appealing from the Office action mailed 03/22/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20010007120	MAKITA	07-2001
6735700	FLINT et al.	05-2004
6272533	BROWNE	08-2001

(9) Grounds of Rejection

The rejection under the first paragraph of 35 USC 112 has been withdrawn.

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 2, 4-7, 10-18, 20-23 and 26-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700.

As per claims 1 and 17, the applicant describes a method for scanning data read from storage comprising the following limitations which are met by Makita in view of Flint:

a) receiving a request for data saved in storage from a central processing unit (Makita: [0180]);

b) scanning the requested data for malicious code (Makita: [0182]);

c) transmitting the data from the storage to the central processing unit if malicious code is not found in the data during scanning (Makita: [0184]);

d) wherein the scanning is performed by a scanning module coupled to a storage subsystem controller (Makita: [0091] and Fig 15);

e) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module (Flint: Col 9, lines 5-24).

The applicant has incorporated original claim 3 into part d) above and original claims 8 and 9 into part e). Makita describes all the limitations of parts a) through d) above. As per part d), the storage subsystem controller is the file management unit (211 of Fig 15) which is coupled to the virus scan unit (413) of Fig 15. The central processing unit pertains to the CPU on the host computer (110 of Fig 15).

Makita does not describe disabling the scanning module. Makita does describe, as discussed in the first office action, that other functions such as formatting can be enabled or disabled by the user (Makita: [0057] and [0058]). However, Makita never discloses that the scanning module can be enabled or disabled by the user.

Flint discloses a similar virus scanning system in which the user can enable or disable the scanning module at will. Being able to enable or disable the scanning module is an obvious improvement because it allows for data to be transmitted efficiently without a scan when the user is sure that data is virus-free or when the user does not care to invest the time to make sure that data is virus free. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Flint with those of Makita and make the virus scanner capable of being disabled or enabled by the user for the case of efficiency when the scanner is not needed.

As per claims 2 and 18, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage is selected from the group consisting of a hard drive, a compact disc-read only memory (CD-ROM), and a floppy disc (Makita: [0004], [0015], and Fig 4);

As can be seen in the paragraphs and figure referenced above, the storage of Makita is a hard drive.

As per claims 4, 20, and 38, the applicant describes the method of claims 1,17, and 35, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate there through (Makita: Fig 15 and [0010]);

According to the applicant's specification, the storage driver "interfaces with the operating system running on the cpu for communicating read and write requests to the storage subsystem controller" (applicant: page 8). The storage driver is the interface unit (21 of Fig 15), the storage subsystem controller is the file management unit (211 of Fig 15), and the CPU is the CPU on the host computer (110 of Fig 15). All of these components are coupled together as illustrated in Fig 15.

As per claims 5 and 21, the applicant describes the method of claims 3 and 19, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage subsystem controller is coupled to the storage (Makita: Fig 15);

The applicant should note as described above, the storage subsystem controller is the file management unit (211 of Fig 15).

As per claims 6-7 and 22-23, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning module includes software (Makita: [0213] and Fig 15);

The primary reference discloses a scanning module unit which incorporates both software and hardware components. Regarding the software component, the primary reference discloses that the virus check can take the form of a program [0213]. Regarding the hardware component, the primary reference discloses the use of a segregated virus check unit which is connected to a plurality of other units, such as a storage unit (22 of Fig 15) and an interface unit (21 of Fig 15) in a bus-style system.

As per claims 10 and 26, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Further comprising executing an event based on results of the scanning [0183];

Two events are mentioned: halting the scanning/transmission of data process and alerting the user.

As per claims 11 and 27, the applicant describes the method of claims 10 and 26, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the event includes an alert (Makita: [0183]).

As per claims 12 and 28, the applicant describes the method of claims 10 and 26, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Further comprising disabling the scanning module in response to the event (Makita: [0183]);

The applicant should note that the scanning/transmission of data process is halted.

As per claims 13 and 29, the applicant describes the method of claims 12 and 28, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein data is precluded from being transmitted from the storage to the central processing unit upon disabling of the scanning module (Makita: [0183]);

As per claims 14 and 30, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning includes content scanning (Makita: [0054] and [0055]);

The applicant should note that the primary reference includes the use of content scanning, which is used to determine a format of data and format the data to a user-selected format, and virus scanning, which is used to detect malicious data.

As per claims 15 and 31, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of

Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning includes virus scanning (Makita: [0182]);

As per claims 16 and 32, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage is accessible via a network (Makita: [0036] and [0196] and Fig 19);

As described by the applicant, the system takes place in "an environment in which the storage device is connected to and/or disconnected from each of a plurality of host computers" [0036].

As per claims 33 and 34, the applicant describes a method for scanning data written to storage comprising the following limitations which are met by Makita in view of Flint:

a) receiving a request for data to be written in storage, the request being received from a central processing unit (Makita: [0174]);

b) scanning the data for malicious code (Makita: [0174]);

c) writing the data to the storage if malicious code is not found in the data during the scanning (Makita: [0177]);

d) wherein the scanning is performed by a scanning module coupled to a storage subsystem controller (Makita: [0091] and Fig 15);

e) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module (Flint: Col 9, lines 5-24);

For motivation for combining the ideas of Makita with those of Flint, see the rejection for claim 1.

As per claims 35 and 39, the applicant describes a system for scanning data read from storage comprising the following limitations which are met by Makita in view of Flint:

a) storage for saving data therein (Makita: 22 of Fig 15);

b) a storage subsystem controller coupled to the storage for controlling access to the data saved therein (Makita: 211 of Fig 15);

c) a central processing unit coupled to the storage subsystem controller for issuing read requests for reading the data saved therein for processing purposes, and write requests

for writing data to the storage (Makita: 110 of Fig 15; 14 of Fig 4; [0008]);

d) a scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests (Makita: 413 of Fig 15);

e) an event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning (Makita: 211 of Fig 15; [0183]; [0091]);

f) wherein the central processing units is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning (Makita: [0183] and [0184]);

g) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module (Flint Col 9, lines 5-24);

As described earlier by the examiner, regarding the use of a central processing unit, the primary reference discloses an

operating system control unit. The operating system control unit embodies the CPU as it is well known in the art that an operating system runs on the central processing unit. The role of the operating system control unit of the primary reference is identical to the role of the CPU as described in the applicant's invention. The operating system control unit controls the read and write requests which take place between the host computer and the remote storage ([0008] and Fig 4). According to the applicant, the central processing unit issues read and write requests between the computer and the storage (Page 5).

Regarding part e), the file management unit acts as the event manager module in addition to acting as the storage subsystem controller. The file management unit controls the transmission between the storage and the host computer [0091]. When a virus is detected, transmission between the remote storage and the host computer is halted [0183]. Since the file management unit executes the security event of halting the transmission between the storage and the host computer, the file management unit acts as the event manager module.

For motivation for combining the ideas of Flint with those of Makita see the rejection for claim 1.

As per claim 36, the applicant limits the system of claim 35, which is anticipated by Makita in view of Flint (see above), with the following limitation which is also met by Makita:

Wherein the scanning module is coupled to the storage subsystem controller via a bus (Makita: Fig 15);

Makita discloses a connection between the scanning module, or virus check unit (413 of Fig 15), and the storage subsystem controller, or file management unit (211 of Fig 15) in a bus configuration where data is transferred between the segregated units.

As per claim 37, the applicant limits the system of claim 35, which is anticipated by Makita in view of Flint (see above), with the following limitation which is also met by Makita:

Wherein the scanning module is directly coupled to the storage subsystem controller (Makita: Fig 15).

The scanning module is 413 of Fig 15 and the storage subsystem controller is 211 of Fig 15.

As per claim 40, the applicant describes the method of claim 1, which is met by Makita in view of Flint (see above), with the following limitation which is also met by Flint:

Wherein the user includes a remote administrator (Flint: Col 2, lines 19-20);

Flint discloses the idea that a user can be an administrator.

Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Makita in view of Flint in further view of Browne, U.S. Patent No. 6,272,533.

As per claim 41, the applicant describes the method of claim 1, which is met by Makita in view of Flint (see above), with the following limitation which is met by Browne:

Wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage (Browne: Col 4, lines 61-64);

Makita in view of Flint discloses all the limitations of independent claim 1. However, Makita in view of Flint fail to disclose any method for preventing data to be transmitted from storage by a user.

Browne discloses a secure computing system in which a manual switch (which is operated by a user) can be pressed so that data is precluded from being written to a storage device.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Browne with those of Makita in view of Flint and add a manual switch to prevent the writing of data to a storage location for security reasons in the event that a user may not want the CPU to write data to the storage device.

New Grounds of Rejection

Claims 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Makita in view of Flint in further view of Browne, U.S. Patent No. 6,272,533.

As per claims 42 and 43, the applicant describes the method of claim 41, which is met by Makita in view of Flint (see above), with the following limitation which is also met by the combined references: wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled (Flint: column 9 lines 5-39 in view of Browne column 4 lines 61-64) and the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central processing unit (Browne: column 4 lines 61-64).

Claims 17, 18, 20-23, 26-32, 34, and 39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 17, 18, 20-23, 26-32, and 34 relate to a computer program product and claim 39 relates to a system with different means plus function language. The computer program products are merely computer code and the specification allows the means to be merely software, therefore these claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material per se.

(10) Response to Argument

Issue #1: Rejection of claims 42-43 under 35 USC 112, first paragraph, has been withdrawn and is no longer on appeal.

Issue #2: Rejection of claims 1, 2, 4-7, 10-18, 20-23 and 26-40 under 35 USC 103(a) as being unpatentable over Makita in view of Flint.

Group #1: Appellant argues the combined references (specifically Flint) fail to teach the claimed limitation of

"data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module".

With respect to this argument, Flint teaches disabling a virus scanner (see column 9 lines 10-15), when the virus scanner is stopped (i.e. disabled) the session stamp of the file is invalidated (see column 9 lines 3-4). Now referring to figure 6, number 611, the session stamp is checked to determine whether it is valid or not, when it is not, the file is scanned for viruses and the session stamp is updated, since the virus scanner is stopped at this point the session stamp is updated to state that it is still invalid as described in column 9 lines 3-4. Now referring to figure 8, which related to the specifics of when the virus scanner is terminated, the virus scanning program and method is stopped without updating the session stamp to be valid therefore when attempting to access this file the above steps will be repeated as long as the virus scanner is off so the session stamp will never be validated and therefore the file cannot not be accessed as further described with respect to figure 7 and column 10 lines 20-32).

Group #2: Appellant argues the references (specifically Makita) do not teach the limitation of a "scanning module coupled to the central processing unit and the storage subsystem

controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests".

With respect to this limitation, Appellant first argues that supplying information to a virus check unit does not meet "a scanning module adapted for identifying requests from the central processing unit", however, in Makita the CPU of the host computer sends a command (i.e. request) for access to a file (see paragraph 180), and the file is then accessed and scanned for viruses (see paragraphs 181 and 182). Therefore, the external storage unit (410 of figure 15) contains a system that receives and identifies requests for data, which is also scanned. Appellant next argues that Makita fails to teach the modules adapted for receiving scanning results and executing an event based on the results. However, as described in paragraphs 183 and 184 the data transmission is either stopped or allowed to continue to the host computer based on the results of virus scanning. Therefore a portion of the external storage unit (410) receives the results and another portion causes an event to happen (stopping or allowing transmission to the host) based on those results.

Group #3 and Group #4: Appellant argues Makita does not teach the scanning module includes software and that Makita does not teach the scanning module includes hardware.

With respect to Appellants arguments that Makita does not teach a scanner includes neither software nor hardware; all virus scanners are a combination of software and hardware for it to run on. Furthermore, the combined reference of Flint teaches a virus program (i.e. software) and this program is tied to a CPU and disk (see column 1 lines 36-50).

Group #5: Appellant argues the combined references fail to teach disabling the scanning module in response to an event.

With respect to this argument, Makita teaches the disabling of functionality based on an event in paragraph 183 (the stopping of transmission based on the virus scanning results) and Flint teaches disabling a virus scanner based on user input (i.e. an event) (see column 9 lines 10-13). Therefore the combination teaches disabling the scanning module in response to an event.

Group #6: Appellant argues Makita fails to teach the scanning includes content scanning.

With respect to this argument, the virus check unit scans the requested file to check if the file contains any known

viruses (scanning for content). Therefore, Makita teaches content scanning.

Group #7: Appellant argues the combined references fail to teach a remote administrator can disable the scanning module.

With respect to this argument Flint teaches that a user can disable a virus scanner (see column 9 lines 10-13). Flint further teaches that user can be an administrator (see column 2 lines 19-20). Therefore, when combined with the remote requests of Makita the combined references teach a remote administrator can disable the scanning module.

Issue #3: Rejection of claim 41 under 35 USC 103(a) as being unpatentable over Makita in view of Flint and further in view of Browne.

Appellant argues that Browne fails to disclose a user is allowed to disable the storage, and the data is precluded from being transmitted to the storage upon said disabling.

With respect to this argument, Browne teaches the use of a read mode that is user activated (see column 4 lines 51-64) and when in read mode data cannot be written to the storage device (see column 8 lines 65-67 “read only”). Therefore, Browne discloses a user is allowed to disable the storage, and the data is precluded from being transmitted to the storage upon said disabling.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Michael Pyzocha/
Patent Examiner, Art Unit 2137
May 28, 2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Benjamin Lanier
/Benjamin E Lanier/
Primary Examiner, Art Unit 2132

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

/ANDREW H HIRSHFELD/
Director, TC 2100